แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Linux และ Oracle ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ

วันที่แจ้งเตือน 1 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Linux และ Oracle ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์ หลายรายการ ได้แก่

ผู้ผลิต/ระบบ	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Linux	• **ช่องโหว่ CVE-2026-43503** ใน Linux Kernel เป็นช่องโหว่ประเภท Local Privilege Escalation (LPE) เกิดจากความผิดพลาดในการจัดการหน่วยความจำของ Kernel ในส่วนของ socket buffers (skb) และ shared page-cache memory ซึ่งใช้เก็บข้อมูลที่เชื่อมโยงกับไฟล์บนดิสก์ เป็นผลให้ผู้โจมตีที่มีสิทธิ์เข้าถึงระบบภายในเพื่อยกระดับสิทธิ์เป็น root ได้ ทำให้สามารถควบคุมระบบได้ เช่น อ่านหรือแก้ไขข้อมูลสำคัญ สร้างบัญชี ผู้ใช้ใหม่ เป็นต้น • Linux Distribution แนะนำให้อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้	ส่งผลกระทบต่อ Linux หลาย distribution เช่น SUSE, Ubuntu, Debian และ Red Hat Enterprise Linux 9 และ 10
	• **ช่องโหว่ CVE-2026-46331** ใน Linux Kernel เป็นช่องโหว่ประเภท Out-of-Bounds Write ในฟังก์ชัน tcf_pedit_act() ของโมดูล act_pedit ซึ่งใช้เพื่อแก้ไขข้อมูลแพ็กเกจเครือข่าย ทำให้ผู้ไม่หวังดีอาจใช้ช่องโหว่ดังกล่าวแก้ไขข้อมูลในสำเนาของไฟล์ที่จัดเก็บไว้ในหน่วยความจำ (Cached) จะฝัง pay load และสั่งรันโปรแกรมที่ถูกสร้างขึ้นด้วยสิทธิ์ระดับสูง เป็นผลให้สามารถควบคุมและซ่อนตัวในระบบโดยตรวจจับได้ยาก • Linux Distribution แนะนำให้อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้	ส่งผลกระทบต่อ Linux หลาย distribution ได้แก่ Red Hat 8 - 10, Debian 11 - 12 และ Ubuntu 18.04, 20.04, 22.04, 23.04, 24.04 และ 26.04

ข้อมูลอ้างอิง CVE-2026-43503

1. https://nvd.nist.gov/vuln/detail/CVE-2026-43503
2. https://research.jfrog.com/post/dissecting-and-exploiting-linux-lpe-variant-dirtyclone-cve-2026-43503/
3. https://securityaffairs.com/194338/uncategorized/dirtyclone-fourth-linux-kernel-flaw-in-six-weeks-escalates-to-root.html

ข้อมูลอ้างอิง CVE-2026-46331

1. https://nvd.nist.gov/vuln/detail/CVE-2026-46331
2. https://github.com/sgkdev/packet_edit_meme
3. https://thehackernews.com/2026/06/new-linux-pedit-cow-exploit-enables.html

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Linux และ Oracle ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ

วันที่แจ้งเตือน 1 กรกฎาคม 2569

ผู้ผลิต/ระบบ	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Oracle	• ช่องโหว่ **CVE-2026-46817** ในผลิตภัณฑ์ Oracle E-Business Suite (EBS) ซึ่งถูกใช้โจมตีจริง เป็นช่องโหว่ในส่วน File Transmission ของผลิตภัณฑ์ Oracle Payments ทำให้ผู้ไม่หวังดีสามารถเข้าสู่ระบบได้โดยข้ามผ่านการยืนยันตัวตน (Un-authentication) และสามารถเข้าควบคุมระบบ Payments ดังกล่าวได้ • Oracle แนะนำให้อัปเกรดผลิตภัณฑ์เป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อผลิตภัณฑ์ Oracle Payments เวอร์ชัน 12.2.3 - 12.2.15

ข้อมูลอ้างอิง CVE-2026-46817

1. https://nvd.nist.gov/vuln/detail/CVE-2026-46817
2. https://www.oracle.com/security-alerts/cspumay2026verbose.html
3. https://www.bleepingcomputer.com/news/security/new-oracle-e-business-suite-flaw-now-exploited-in-attacks/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ